UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,558	08/16/2001	Massimiliano Antonio Poletto	12221-009001	4255

26161 7590 10/19/2005

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,558	POLETTO ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/28/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the RCE filed 07/28/2005. Claims 2-4 and 11 have been amended. The specification has also been amended.

Response to Amendment

2. Claim 2, which is "currently amended", is not presented with marking(s) to indicate the change(s) that have been made relative to the immediate prior version. Appropriate correction is required.

3. Claim 11, which has been changed, but is not indicated as being "currently amended". Appropriate correction is required.

4. The Applicant has indicated the paragraph beginning at page 4, line 24 to be replaced with the amended paragraph filed 07/28/2005. However, the paragraph to be replaced begins at page 5, line 3 of the Specification. Appropriate correction is required.

Response to Arguments

5. Applicant's arguments filed 07/28/2005 have been fully considered but they are not persuasive. Applicant argues that it would not be suggestion to one of ordinary skill in the art, to modify Mansfield with Mell to provide the claimed feature of a port to link the data collector over a redundant network that does not carry the packet traffic to

deliver the accumulated and collected statistical information about the network packet traffic to a central control center (page 9, 1st paragraph). Mell discloses a system comprising data collectors (i.e. IDS nodes) collecting data from network traffic and sending the collected data to a central control center (i.e. the command and control system at the root) (Section 2.0). Mell also discloses the vulnerability of such a system is that an IDS node can be cut off from the system due to a denial-of-service attack on that particular IDS node. Mell further discloses a known solution and his own solution to the problem: "one solution to this problem is to provide IDSs a separate and protected communication channel for their operation. This solution works well but very costly ... Our solution using mobile agents ... However, our solution has its own set of requirements and assumptions" (Section 3.0). According to Mell, the known solution, though costly, works well. On the other hand, Mell's solution of using mobile agents, though not as costly, has security drawbacks and problems (Section 4.0). It's obvious that Mell's solution is just an alternative to the known solution, each having its own advantage(s) and disadvantage(s). It is well known in the art of network security that there often is more than one solution to a security problem and that a solution is selected based on a particular system's security requirement, performance and/or cost. Therefore, for a system that does not tolerate security compromises and where cost is not an issue, it would be obvious to one of ordinary skill in the art to select the known solution of using a separate communication channel.

Applicant argues that Mansfield does not suggest that the data collectors deliver the accumulated and collected statistical information to the control center (page 10, 1st

paragraph). Mansfield discloses different data collectors monitor traffic pattern at different locations in a network and the NMS compares the monitored traffic patterns and correlates them (Section 3.1).

Applicant argues that Mansfield does not disclose dividing the traffic flow into buckets that track counts of how many packets a data collector examines for a given parameter (page 12, 3rd paragraph). Mansfield discloses dividing the traffic flow into different categories and using memory spaces to track counts of how many packets a data collector examines for a given parameter (page 4, last paragraph). A bucket can be implemented in different ways and since Mansfield uses memory spaces to track counts of packets for a given parameter, the memory spaces meet the limitation of buckets. Applicant argues that Zait only discloses hash-based partitioning and range-based partitioning but does not disclose adjusting the number of buckets by combining several buckets into fewer buckets or dividing a bucket into more buckets and there is no suggestion to combine the reference (page 12, last paragraph). A partition is a bucket and Zait discloses adjusting the number of buckets by dividing a bucket into smaller buckets and provides motivation to combine the reference (col. 10, lines 16-37). In addition, it is the claimed invention that also uses the hash-based partitioning method to divide the traffic flow into buckets (Specification, page 16, 2nd paragraph).

Applicant argues that Roesch does not disclose monitoring for unusual level of IP fragmentation (page 13, last paragraph). Roesch discloses that IP fragmented packet probes and attacks can be logged and alerts can be sent automatically (p. 230, right col., "Snort currently addresses IP fragmentation ... sent by Snort automatically").

Applicant argues that Eichstaedt does not provide any suitable motivation and that Eichstaedt is of no import to an intrusion detection (page 14, 4th paragraph). Eichstaedt is relied upon for the teaching of the claimed feature as well as the motivation for combining the references (col. 1, lines 49-63; col. 3, lines 3-7; col. 6, lines 20-33).

Applicant argues that Stalling has no relevant teachings related to statistical data (page 15, 4th paragraph). Stalling discloses that a LAN monitor agent audits host-host connections, services used and volume of traffic to detect anomalies in network load, network activities and security-related services (page 500, 3rd paragraph). Stalling further discloses different statistical anomaly detection techniques (page 494).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-3, 5-8, 10-13, 15, 17-19 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield ("Towards Trapping Wily Intruders in the Large") in view of Mell et al ("Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems").

Regarding claims 1-3, 11 and 21, Mansfield discloses a method for a data collector to collect data from sampled network traffic comprising: sampling packet traffic over a network and generating statistical information about the packet traffic on the network (Section 3, Detection of Intrusions from traffic-flow signatures; Section 5, Implementations and Results); parsing the information in the sampled packets and maintaining the information in a log (Section 3, Detection of Intrusions from traffic-flow signatures); and delivering the generated statistics over a network to a central control center (Section 5, Implementations and Results; Section 3.1, Traffic-flow signature).

Mansfield does not disclose utilizing a redundant network that does not carry the packet traffic to deliver the generated statistics to a central control center. Mell discloses utilizing a separate and protected network for communications between data collectors and a control center (Section 2.0, Background on Distributed Hierarchical IDSs; Section 3.0, Vulnerable Systems). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mansfield method to utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing.

Regarding claim 5, Mansfield further discloses that the information collected by the data collector includes source information and destination information (Table 1; Section 3, Detection of Intrusions from traffic-flow signatures).

Regarding claim 6, Mansfield further discloses that the data collector collects the information but does not log the sampled packets (Section 3.1, Traffic-flow signature).

Regarding claim 7, Mansfield further discloses that the data collector analyzes the collected statistics and produces a message that raises an alarm to the control center (Section 5, Implementations and Results).

Regarding claims 8 and 22, Mansfield further discloses that the data collector includes a communication process to respond to queries from the control center for information concerning characteristics of packet traffic on the network (Section 5, Implementations and Results).

Regarding claim 10, Mansfield further discloses that the query can be a request to download via the redundant network, a portion of a log of the collected information (Section 5, Implementations and Results) maintained by the data collector.

Regarding claim 12, Mansfield further discloses monitoring packet count, which is a parameter of traffic flow, at two levels of granularity (p. 5, 1st par., "The initial threshold will need ... ball rolling"; Section 3.2, Definition of traffic-flow signature).

Regarding claim 13, Mansfield further discloses that monitoring the parameter at multiple levels of granularity is used to trace the source of an attack (Section 5, Implementations and Results).

Regarding claim 15, Mansfield further discloses applying multi-level analysis monitor TCP packet ratios, repressor traffic and statistics based Layer 3-7 analysis (Section 3.3, Correlating traffic-flow signatures; Section 4, Map-based distributed Intrusion tracing; Table 1; Section 2, Characteristics of Network Intrusions).

Regarding claim 17, Mansfield further discloses monitoring network traffic for ICMP packets with broadcast destination addresses (Section 3.4, Experimental evaluation).

Regarding claim 18, Mansfield further discloses monitoring network traffic protocol (TCP) or user datagram protocol (UDP) packets addressed to unused ports (Table 1).

Regarding claim 19, Mansfield further discloses monitoring network traffic for transmission control protocol (TCP) ACK packets that do not belong to a known connection (Section 4, Map-based distributed Intrusion tracing).

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell. Mell discloses using a dedicated line (Section 3.0, Vulnerable Systems). Mell does not disclose that the dedicated line is a leased line. However, Examiner takes Official Notice that using a leased line as a dedicated line is well known in the art. It would have been obvious at the time of the invention was made to use a leased line as a dedicated line since using a leased line as a dedicated line so that there is no need to build and/or maintain a network is well known in the art.

9. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell as applied to claim 13 above, and further in view of Zait et al (6,665,684). Mansfield discloses dividing the traffic flow and using memory spaces to track counts of how many packets a data collector examines for a given parameter (p.

5, 1st par., "The initial threshold will need ... ball rolling"). The memory spaces meet the limitation of buckets. Mansfield does not disclose adjusting the number of buckets as the number of buckets approaches a bucket threshold, by combining several buckets into fewer buckets or dividing a bucket into more buckets. Zait discloses adjusting the number of buckets as the number of buckets approaches a threshold, by dividing a bucket into more buckets (col. 10, lines 25-32). Mansfield and Zait are analogous art because they are from a similar problem solving area, efficient storing and searching for data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Mell to adjust the number of buckets as the number of buckets approaches a threshold, by dividing a bucket into more buckets, as taught by Zait, so that the granularity level matches a degree of parallelism when the degree of parallelism exceeds a threshold.

10. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell as applied to claim 15 above, and further in view of Roesch ("Snort-Lightweight Intrusion Detection for Networks"). Mansfield and Mell do not disclose monitoring network traffic for fragmented IP packets. Roesch discloses monitoring network traffic for fragmented IP packets (p. 230, right col., "Snort currently addresses IP fragmentation ... sent by Snort automatically"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Mell to monitor network traffic for fragmented IP

packets, as taught by Roesch, so that fragmented packet probes and attacks could be logged and alerts could be generated.

11. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell as applied to claim 15 above, and further in view of Eichstaedt et al (6,662,230). Mansfield and Mell do not disclose monitoring network traffic generated not by a human user over a persistent HTTP connection. Eichstaedt discloses monitoring network traffic generated not by a human user over a persistent HTTP connection (col. 1, lines 49-63; col. 3, lines 3-7; col. 6, lines 20-33). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Mansfield and Mell to monitor network traffic generated not by a human user over a persistent HTTP connection, as taught by Eichstaedt, in order to prevent overcrawling by robots that make too frequent requests.

12. Claims 1-3, 5-8, 10-13 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings ("Cryptography And Network Security: Principles and Practice") in view of Mell.

Regarding claims 1-3, 11 and 21, Stallings disclose a method for a data collector to collect data from sampled network traffic comprising: sampling packet traffic over a network and generating statistical information about the packet traffic on the network (p. 499, "One or more node ... could be valuable"; p. 500, "The LAN monitor agent ... activities such as rlogin"; figures 15.5 and 15.6; p. 494, "Statistical Anomaly Detection");

parsing the information in the sampled packets and maintaining the information in a log (p. 499, "The scheme is designed ... host audit record (HAR)"); and delivering the generated statistics over a network to a central control center (fig. 15.6).

Stallings does not disclose utilizing a redundant network that does not carry the packet traffic to deliver the generated statistics to a central control center. Mell et al ("Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems") discloses utilizing a separate and protected network for communications between data collectors and a control center (Section 2.0, Background on Distributed Hierarchical IDSs; Section 3.0, Vulnerable Systems). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Stallings method to utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing.

Regarding claim 5, Stallings further discloses that the information collected by the data collector includes source information and destination information (p. 500, "The LAN monitor agent ... such as *rlogin*").

Regarding claim 6, Stallings further discloses that the data collector collects the information but does not log the sampled packets (p. 500, "The LAN monitor agent ... such as *rlogin*").

Regarding claim 7, Stallings further discloses that the data collector analyzes the collected statistics and produces a message that raises an alarm to the control center (p. 500, "When suspicious activity is detected ... from other agents").

Regarding claims 8 and 22, Stallings further discloses that the data collector includes a communication process to respond to queries from the control center for information concerning characteristics of traffic on the network (p. 500, "When suspicious activity is detected ... from other agents"; fig. 15.6).

Regarding claim 10, Stallings further discloses that the query can be a request to download via the redundant network, a portion of a log of the collected information (p. 499, "One or more nodes ... information could be valuable"; fig. 15.6).

Regarding claim 12, Stallings further discloses monitoring a parameter of traffic flow at different levels of granularity (p. 495, "The simplest statistical test ... and resource measures").

Regarding claim 13, Stallings further discloses that monitoring the parameter at multiple levels of granularity is used to trace the source of an attack (p. 500, "At the lowest level ... file accessed, and the like").

Regarding claim 14, Mell does not disclose that the dedicated line is a leased line. However, Examiner takes Official Notice that using a leased line as a dedicated line is well known in the art. It would have been obvious at the time of the invention was made to use a leased line as a dedicated line since Examiner takes Official Notice that using a leased line as a dedicated line so that there is no need to build and/or maintain a network is well known in the art.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,792,546 to Shanklin et al.

Honeypots.net, "Intrusion Detection, Honeypots and Incident Handling Resources"

Jackson, "Intrusion Detection System (IDS) Product Survey"

Wood, "Intrusion Detection Message Exchange Requirements – Internet Draft"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

10/07/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100